Стахановец

Признаки внутреннего нарушителя

Чек-лист для служб информационной безопасности

Внутренний нарушитель редко проявляется одним ярким событием. Чаще это набор мелких сигналов в действиях с данными и системами. Ниже — на что смотреть в первую очередь. Отдельный признак ещё не обвинение: важна совокупность сигналов и их проверка.

Для субъектов КИИ внутренний нарушитель не абстрактный риск: Методика оценки угроз ФСТЭК России выделяет его как отдельный тип источника угроз. На значимых объектах внешний периметр обычно закрыт хорошо, а вот действия людей с легальным доступом: администраторов, инженеров, подрядчиков — часто остаются вне поля зрения. Поэтому под каждой группой признаков указаны меры Приказа № 239, к реализации которых они относятся.

1. Работа с данными и файлами

Меры Приказа ФСТЭК № 239: АУД.4 «Регистрация событий безопасности», АУД.9 «Анализ действий отдельных пользователей»

- ☐ Массовое копирование или выгрузка файлов, не связанные с текущими задачами
- ☐ Сбор данных «про запас», архивирование больших объёмов информации
- ☐ Обращение к документам и базам за пределами своей зоны ответственности
- ☐ Запароленные архивы или шифрование файлов перед их передачей
- ☐ Хранение чувствительных данных локально, вне защищённых хранилищ

2. Каналы передачи информации

Меры Приказа ФСТЭК № 239: ЗИС.17 «Защита информации от утечек», ЗНИ.5 и ЗНИ.6 (контроль съёмных носителей), АУД.5 «Контроль и анализ сетевого трафика»

- ☐ Отправка рабочих документов на личную почту
- ☐ Загрузка файлов в личные облачные хранилища и мессенджеры
- ☐ Копирование данных на личные USB-накопители и внешние диски
- ☐ Массовая или выборочная печать конфиденциальных документов
- ☐ Фотографирование экрана на телефон

3. Доступ и обход защиты

Меры Приказа ФСТЭК № 239: АУД.7 «Мониторинг безопасности», ОПС.1 и ОПС.2 (управление запуском и установкой ПО)

- ☐ Попытки получить права и доступы сверх необходимых для работы
- ☐ Использование чужих учётных записей или передача своих паролей
- ☐ Попытки отключить или обойти средства защиты и мониторинга

- ☐ Использование анонимайзеров и средств сокрытия активности
- ☐ Интерес к системам и данным вне своей компетенции

4. Поведение и время работы

Меры Приказа ФСТЭК № 239: АУД.9 «Анализ действий отдельных пользователей», АУД.7 «Мониторинг безопасности»

- ☐ Регулярная работа в нерабочее время без производственной необходимости
- ☐ Резкий рост активности с данными перед увольнением или отпуском
- ☐ Действия, не совпадающие с обычным рабочим профилем сотрудника
- ☐ Систематическое нарушение внутренних политик безопасности

5. Контекст (учитывать с осторожностью)

Организационные факторы — прямой привязки к мерам приказа не имеют.

- ☐ Открытый конфликт с работодателем или явное недовольство
- ☐ Известный предстоящий уход, особенно к конкуренту
- ☐ Внешние связи с конкурентами или подозрительные контакты

Контекстные признаки сами по себе ничего не доказывают — это лишь повод внимательнее отнестись к техническим сигналам из разделов 1–4.

Соответствие указано ориентировочно: конкретный набор мер зависит от категории значимости объекта и модели угроз. Например, ЗИС.17 не входит в базовый набор ни для одной категории и применяется при дополнении набора по результатам моделирования угроз, а АУД.9 и АУД.5 базовые только для объектов 1 категории.

Хотите увидеть, какие из этих признаков проявляются в вашей инфраструктуре?
Запросить демонстрацию «Стахановец» →

Как это отслеживать

Отметить пункты в этом списке — только первый шаг. Вручную такие сигналы не отследить: они разрознены, приходят из разных источников и заметны лишь в совокупности. Эту работу берёт на себя система контроля действий персонала — единый журнал событий, поведенческая аналитика и оповещения о нарушениях политик.

Важно

- Ни один признак сам по себе не является доказательством: важна совокупность сигналов и их проверка.
- Реагировать следует через установленные процедуры, а не через поспешные выводы в отношении конкретного сотрудника.
- Порядок контроля нужно закрепить в локальных нормативных актах и ознакомить с ними работников под подпись.

- В правилах стоит прямо запретить использование рабочих устройств и корпоративной почты в личных целях: тогда у сотрудника не возникает разумного ожидания приватности в рабочем канале.
- Контроль ограничивается рабочим временем и рабочими устройствами — сбор данных о частной жизни недопустим (ст. 23 Конституции РФ, ст. 137 и 138 УК РФ).
- Собранные сведения о работниках — это персональные данные: их обработка и хранение подчиняются 152-ФЗ, а доступ к записям должен быть ограничен.